非線形量子計算の模倣における領域量について (計算機科学の基礎理論 : 21世紀の計算パラダイムを目指して)

AUTHOR(S):

金田, 直樹; 西野, 哲朗

CITATION:

金田, 直樹 ...[et al]. 非線形量子計算の模倣における領域量について (計算機科学の基礎理論 : 21世紀の計算パラダイムを目指して). 数理解析研究所講究録 2000, 1148: 52-57

ISSUE DATE:

2000-04

URL:

http://hdl.handle.net/2433/64015

数理解析研究所講究録
1148巻 2000年 52-57

非線形量子計算の模倣における領域量について

金田　直樹 (Kanada Naoki)　　西野　哲朗 (Nishino Tetsuro)

電気通信大学大学院 電気通信学研究科

〒182-8585 東京都調布市調布ヶ丘 1-5-1
e-mail: {kanada,nishino}@ice.uec.ac.jp

1　はじめに

量子計算は，量子力学の基本原理である重ねあわせの原理，ユニタリな時間発展，確率解釈のうち，重ねあわせの原理を用いて計算を高速化しようという試みである．具体的には，量子 Turing 機械 (以下，QTM と略記する) という計算モデルにおいて，各セルが 0 と 1 の重ね合わせ状態 $\alpha|0\rangle+\beta|1\rangle$ を保持できるものと仮定する．P. W. Shor はこのような仮定をおいたときに離散対数および因数分解問題を解く誤り限定量子多項式時間アルゴリズムを構成できることを示し，注目を集めた [8]．その後にも，L. K. Grover によりデータベース検索に対する量子アルゴリズムがなど得られた [5]．

このような量子計算の枠組みは，D. Deutsch により導入された．論文 [4] において Deutsch は QTM を定義し，万能 QTM を構成した．しかし，この万能 QTM はある QTM を模倣するときに指数倍の速度低下を必要とするので，現在ではそのようなことのない Bernstein と Vazirani による定義 [3] が QTM の標準的な定義として使われている．

QTM が各セルに 0 と 1 の重ね合わせ状態を保持している場合，n 個のセルに全部で 2^n 個の重ね合わせ状態が保持されており，この重ね合わせ状態に対し QTM は一斉に計算を行うことができる（量子並列化計算）．例えば n 変数ブール式 f に対して，2^n 個の変数割り当てに対する f の値を同時に計算できる．しかし，重ねあわせの原理と同時に要請される確率解釈は，重ね合わせ状態を読み出すときに重ねあわせの比率に応じた確率で，どれか 1 つの重ね合わせ状態のみを読み出せるとしており，単純に計算を高速化できるわけではない．例えば NP 完全問題のような問題では，一般に，計算した重ね合わせ状態内における解の比率が小さくなるので，結果を求めるのに必要な計算と観測回数の増加が量子並列化の効果を相殺してしまう可能性がある．

D. S. Abrams と S. Lloyd は非標準的な枠組みである非線形量子力学から導かれる非線形変換を導入することで任意の NP 完全問題が多項式時間で解けることを示した．我々はすでに SAT を解くための Abrams と Lloyd のアルゴリズムが DTM および QTM を用いて線形領域内で模倣可能であることを示した [9]．本論では最初に Abrams と Lloyd のアルゴリズムを模倣する QTM と，SAT を解く DTM の使用するセルの数についての関係についての結果を示す．次に，Abrams と Lloyd のアルゴリズムで使われる非線形変換はどれも同程度の難しさであることを示す．最後に，Abrams と Lloyd の与えた非線形変換を模倣する QTM と，SAT を解く DTM の使用するセルの数に関する結果を示す．

2　諸定義

文字を元とする有限集合を**アルファベット**という．アルファベット Σ の元を重複を許して有限個並べた列を**文字列**と言い，文字列を構成している文字の個数を文字列の**長さ**と言う．x が文字列のとき，x の長さを $|x|$ と書く．長さ 0 の文字列を**空列**と言い，ε で表す．Σ の **Kleene 閉包** Σ^* を $\Sigma^*=\bigcup_{n\geq 0}\Sigma^n$ と定義し，集合 $S\subseteq\Sigma^*$ を Σ 上

の言語と言う．また，アルファベット $\{0,1\}$ 上の文字列を 2 進列と言う．

定義 1 k **テープ決定性 Turing 機械**とは，以下の条件を満たす 7 項組 $M=\langle Q,\Sigma,\Gamma,\delta,B,q_0,F\rangle$ として定義される．ここで，
Q は**状態**の有限集合，
Γ は**テープ記号**の有限集合，
$B\in\Gamma$ は**空白記号**，
$\Sigma\subseteq\Gamma-\{B\}$ は**入力記号**の有限集合，
$q_0\in Q$ は**初期状態**，
$F\subseteq Q$ は**最終状態**の集合，
$\delta:(Q-F)\times\Gamma^k\to Q\times(\Gamma\times\{L,R\})^k$ は**状態遷移関数**である．

$Q\times(\Gamma^*\times\mathbf{N})^k$ の元を Turing 機械の**様相**と言う．

オフライン k **テープ決定性 Turing 機械**（以下，単に DTM と略記する．特にテープ数を問題にするときには k テープ DTM と略記する．）は，読み出し専用の入力テープと，作業用テープを k 本持つ，$k+1$ テープ決定性 Turing 機械である．i 番目の作業用テープを第 i テープと呼ぶ．k テープ DTM の入力 $a\in\Sigma^*$ は $\not{c}a\$$ の形で入力テープに与えられる．ただし，$\not{c},\$\notin\Sigma$ とする．

定義 2 k **テープ量子 Turing 機械**とは，以下の条件を満たす 7 項組 $M=\langle Q,\Sigma,\Gamma,\delta,B,q_0,F\rangle$ として定義される．ここで，Q は**状態**の有限集合，
Γ は**テープ記号**の有限集合，
$B\in\Gamma$ は**空白記号**，
$\Sigma\subseteq\Gamma-\{B\}$ は**入力記号**の有限集合，
$q_0\in Q$ は**初期状態**，
$F\subseteq Q$ は**最終状態**の集合，
$\delta:(Q-F)\times\Gamma^k\to\tilde{\mathbf{C}}^{Q\times(\Gamma\times\{L,R\})^k}$ はは**状態遷移関数**である．ただし，$\tilde{\mathbf{C}}$ は決定性アルゴリズムを用いて，n ステップ以内に実部と虚部を 2^{-n} の精度で計算可能な複素数 $\alpha\in\mathbf{C}$ の集合とする．

量子 Turing 機械においては，その状態遷移行列のユニタリ性が要請されるが，可逆 Turing 機械はこの要請を満たすことが知られている [3]．論文 [3] においては単テープ量子 Turing 機械のみが扱われていたが，k テープ量子 Turing 機械を $2k$ トラックの単テープ量子 Turing 機械で模倣することにより，k テープ量子 Turing 機械についても同様の議論が成り立つ．多テープ量子 Turing 機械については，[7] でも議論されている．

オフライン k **テープ量子 Turing 機械**（以下，単に QTM と略記する．特にテープ数を問題にするときには k テープ QTM と略記する．）は，読み出し専用の入力テープと，作業用テープを k 本持つ，$k+1$ テープ量子 Turing 機械である．i 番目の作業用テープを第 i テープと呼ぶ．k テープ QTM の入力 $a\in\Sigma^*$ は $\not{c}a\$$ の形で入力テープ上に与えられる．ただし，$\not{c},\$\notin\Sigma$ とする．

QTM の 1 セルに保持される情報量の単位を **qubit** という．本論では，Dirac の記法を用い，あるヒルベルト空間 H 内のベクトル ϕ を表すのにケット記法を用いて $|\phi\rangle$ と表記する．

ある DTM および QTM M が n 個のセルを使用するとは，M の受理計算における任意の時点での任意の重ね合わせ状態において入力テープに対するヘッドを除くすべてのヘッドの位置と最左セルの間の距離が n 以下であることである．

3 Abrams と Lloyd のアルゴリズム

Abrams と Lloyd のアルゴリズムは，量子力学において非線形性を仮定したときに，任意の NP 完全問題を多項式時間で解くアルゴリズムである．本論では，記述を簡潔にするために SAT を解く Abrams と Lloyd のアルゴリズムを AL アルゴリズムと呼び，そのアルゴリズムについてだけ述べる．

以下では，n 個の qubit をまとめて次のように書く．

$$|i_1\rangle|i_2\rangle\cdots|i_n\rangle=|i_1i_2i_3\cdots i_n\rangle$$

これをさらに省略して $|i\rangle\,(0\leq i\leq 2^n-1)$ とも略記する．

また，AL アルゴリズムにおいては $n+1$ 個の qubit を使う．ここで，n は SAT における変数の個数，l を SAT に対する入力のブール式 f の記述長とする．変数割り当てを指定したときに f の評価に必要なステップ数を $h(l)$ とする．$(n+1)$ 番目の qubit を特に “flag qubit” と呼ぶ．flag qubit は，判定問題の結果である “yes” または “no” を

書き込むために用いられる．ブール式 f の n 個の変数 $x_1, x_2, \cdots, x_n$ に値 $i_1, i_2, \cdots, i_n$ を割り当てたときの f の値を $f(i_1, i_2, \cdots, i_n)$ と書き，これを省略して $f(i)$ と書く．ただし，$i = i_1 i_2 \cdots i_n$ とする．また，AL アルゴリズムで使う，2 qubit に対する非線形変換 N を以下のように定義する．任意の 2 qubit を

$$\mathbf{a} = |00\rangle + |11\rangle\,,\ \mathbf{b} = |01\rangle + |10\rangle$$
$$\mathbf{c} = |00\rangle + |10\rangle\,,\ \mathbf{d} = |01\rangle + |11\rangle$$

の 4 つの基底で展開したとき，(2 qubit なので必ず相異なる 4 つの基底によって展開できる．) この 4 つの重ね合わせに対して

$$\begin{aligned}
\mathbf{a} = |00\rangle + |11\rangle \quad &\rightarrow \quad |01\rangle + |11\rangle = \mathbf{d} \\
\mathbf{b} = |01\rangle + |10\rangle \quad &\rightarrow \quad |01\rangle + |11\rangle = \mathbf{d} \\
\mathbf{c} = |00\rangle + |10\rangle \quad &\rightarrow \quad |00\rangle + |10\rangle = \mathbf{c} \\
\mathbf{d} = |01\rangle + |11\rangle \quad &\rightarrow \quad |01\rangle + |11\rangle = \mathbf{d}
\end{aligned}$$

という変換を施す変換を非線形変換 N とする．

この変換において，1 番目の qubit を partner qubit, 2 番目の qubit を flag qubit と呼ぶ．この変換は partner 側はそのままに，flag だけ $|0\rangle + |1\rangle$ から $|1\rangle$ に写像する変換である．

最初に，$n+1$ qubit からなる初期状態 $|\Psi_0\rangle = |00\cdots0\rangle$ を用意する．このとき，AL アルゴリズムとは SAT を解く以下のようなアルゴリズムである．

Phase 1 最初の n bit の可能なすべての 2 進列を等しい確率振幅で重ね合わせた状態を作る．この操作には，QTM 上において n ステップを必要とする．

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{i_1,\cdots,i_n=0}^{1} |i_1 i_2 \cdots i_n, 0\rangle$$

Phase 2 Phase 1 における重ね合わせ状態内の各様相において $f(i)$ を計算し，$n+1$ 番目の qubit にその値を書き込む．$f(i)$ の計算は，QTM において $h(l)$ 時間で行うことができる．ここまでの操作により，以下のような重ね合わせ状態が得られる．

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i, f(i)\rangle$$

Phase 3 Phase 2 の重ね合わせ状態において，先頭の qubit を partner, $n+1$ 番目の qubit を flag qubit として選び，非線形変換 N を作用させる．

Phase 4 Phase 3 と同様の変換を 2 番目の qubit と flag qubit , 3 番目の qubit と flag qubit , $\cdots$, n 番目の qubit と flag qubit の組に対して順次行う．

Phase 5 "yes" か "no" かを判定するために flag qubit を観測する．

2 qubit に対する非線形変換 N が定数ステップで実行できるならば，SAT の解を以上の方法を用いて入力サイズに対する多項式時間で得ることができる．

4 AL アルゴリズムを模倣する DTM の領域量

この節では，AL アルゴリズムを模倣する QTM が使用するセルの数と与えられた n 変数ブール式 f の充足可能性を判定する DTM の使用するセルの数の関係について示す．

定理 3 $k \geq 1$ とし，$g(n) : \mathbf{N} \rightarrow \mathbf{N}$ とする．このとき，非線形変換 $N_n N_{n-1} \ldots N_1$ を模倣する，$g(n)+1$ 個のセルを使用する k テープ QTM M_1 が存在する必要十分条件は，与えられたブール式 f の充足可能性を $g(n)+1$ 個のセルを使用して判定する，k テープ DTM M_0 が存在することである．

証明：DTM M_0 は以下のように動作する．M_0 は f が充足可能であるかどうかを判定し，充足可能なら 1 を，充足不能なら 0 を第 1 テープの先頭に書き込み，停止するものとする．このセルの内容を *flag* と呼ぶことにする．このときの様相を図 1 に示す．

($\leftarrow$ の証明)：以下のように動作する DTM M' を考える．M' で 非線形変換 N を模倣するためには flag qubit を書き換える必要がある．そこで，flag qubit を第 1 テープの先頭にコピーする．その後，M' は第 1 テープの先頭のセル以外の，長

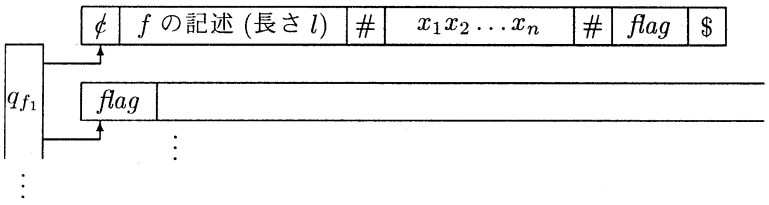

図 1: M_0 が計算を終了して停止したときの様相.

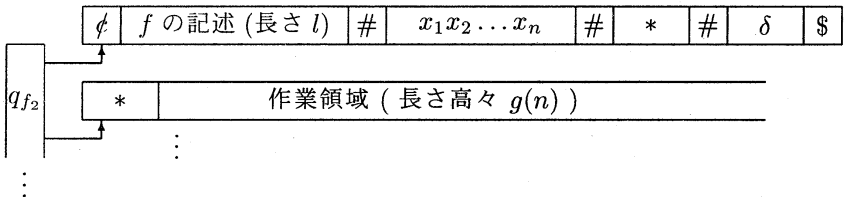

図 2: M_1 が計算を終了して停止したときの様相. ただし, $*$ は flag qubit が書き込まれていることを示す.

さ高々 $g(n)$ の作業領域を使用して M_0 の動作を模倣する. 次に, [2] の手法を用いて, この M' を決定性可逆 Turing 機械に変換する. このようにして得られた決定性可逆 Turing 機械を, [3] の定理 4.2 の手法により模倣する QTM を M_1 と呼ぶ.

この M_1 が非線形変換 $N_nN_{n-1}\ldots N_1$ を模倣していることを示す. $N_nN_{n-1}\ldots N_1$ が終了した時点では, flag qubit には f が充足可能であるときには $|1\rangle$, 充足不能であるときには $|0\rangle$ が書き込まれている. M_0 は f が充足可能であるときに 1 を, 充足不能であるときに 0 を書き込んで停止するとしたので, それから構成された M_1 も f が充足可能であるときに flag qubit に $|1\rangle$ を, 充足不能であるときに flag qubit に $|0\rangle$ を書き込んで停止する.

また, このように構成された M_1 は $g(n)+1$ 個のセルを使用する.

($\rightarrow$ の証明) k テープ QTM M_1 が存在すれば, それを用いて以下のような k テープ DTM M_0 を構成可能であることを示す.

まず, M_1 は非線形変換 $N_nN_{n-1}\ldots N_1$ への入力である, f の記述, 変数 $x_1x_2\ldots x_n$, flag qubit を受け取り, flag qubit を第 1 テープの先頭にコピーする. M_1 はその後, AL アルゴリズムの Phase 3, 4 を模倣する. 模倣が終わった時点における M_1 のテープの内容を図 2 に示す.

M_1 の計算が終了したとき, テープ上の内容は重ね合わせ状態にあるが, その重ね合わせられた様相のうちから, 任意の 1 つを選ぶ. この様相を C_{last} と記す. また, M_1 の動作における C_{last} の 1 ステップ前の様相を $C_{\text{last}-1}$ と記す.

同様に, $C_{\text{last}-1}$ の 1 ステップ前の様相を $C_{\text{last}-2}$, さらに 1 ステップ前を $C_{\text{last}-3}$,... とすると, 最後には重ね合わせられた初期様相のうちの 1 つである C_0 に到達する. このとき, 様相の列 $C_0, C_1, \ldots, C_{\text{last}}$ はある k テープ DTM M が行う計算を表している. これは QTM M_1 の計算を計算木で表したときに, 根と任意の葉の間の任意の道がある DTM の計算に対応していることによる.

このようにして構成した M は, M_1 が AL アルゴリズムを模倣していることより (AL アルゴリズムは f が充足可能であるときに 1 を, 充足不能であるときに 0 を flag qubit に書き込んで停止するので), f が充足可能であるときに 1 を, 充足不能であるときに 0 を *flag* に書き込む. 明かに, M を模倣する k テープ DTM M_0 を構成することができる.

また, M,M_0 の構成法から, M_0 が使用するセルの数は高々 $g(n)+1$ である.

■

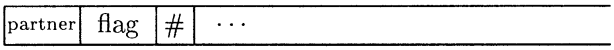

図 3: 非線形変換 N_0 を作用させる作業用テープ.

図 3 のような重ね合わせ状態にある作業用テープにおいて，partner qubit と flag qubit の組に対して行われる非線形変換 N を N_0 と呼ぶ.

定理 4 : $1 \leqq i \leqq n$, $g(n) : \mathbf{N} \to \mathbf{N}$, $g(n) \geqq \lfloor \log_2 n \rfloor + 2$ であるとする．このとき，非線形変換 N_0 を模倣する $g(n)+3$ 個のセルを使用する k テープ QTM M_2 が存在すれば，非線形変換 N_i を模倣する $g(n)+3$ 個のセルを使用する k テープ QTM M_3 が存在する.

証明：M_3 は入力として，長さ l の f の記述，変数の値を表す 2 進列 $x_1 x_2 \ldots x_n$，flag qubit の値，M_2 の状態遷移関数 δ，自然数 i を与えられる．$x_1 x_2 \ldots x_n$ と flag qubit に対応するセルは重ね合わせ状態にある.

以下のように動作する DTM M' を考える．M' はまず，入力テープに記入されている flag qubit を第 1 テープの先頭から 2 番目のセルにコピーする．次に，第 1 テープの前から 3 番目のセルに # を書き込み，その後ろに i をコピーし，さらにその次のセルに # を書き込む．この領域は **counter** として使用される.

次に，M' は入力テープに対するヘッドを x_i の書き込まれているセルに合わせる．このために counter の領域を使用する．まず，M' は入力テープヘッドを x_1 が書かれたセルの左隣のセルに置く．そして，入力テープヘッドを 1 つ右に移動させるごとに counter の値を 1 減らす．したがって，counter が 0 になったときに，M' の入力テープヘッドは x_i を指している．この手法を用い，M' は x_i を第 1 テープの先頭へコピーする．これは flag qubit に対する partner となる．この M' は定理 3 の場合と同様に，ある QTM M'' により模倣することができる.

M_3 はまず M'' の模倣を行う．すなわち，M_2 の状態遷移関数 δ を読んで，M_2 の模倣を行う．(先ほど，counter の書き込まれていた領域は，上書きされる.)

M_3 の使用するテープ上の領域は，partner，flag，# の 3 つの領域と，$g(n)$ 個のセルからなる作業領域である．$g(n)$ の値は (counter の使用する領域) + (counter の右端の # が占める領域) より大きくなければならないので，$g(n) \geqq \lfloor \log_2 i \rfloor + 2$ となり，$i \leqq n$ より $g(n) \geqq \lfloor \log_2 n \rfloor + 2$ となる.

この M_3 は x_i を flag qubit の partner として選び，非線形変換 N を作用させているので，i 番目の非線形変換 N_i の模倣を確かに行っている．■

定理 5 $g(n) : \mathbf{N} \to \mathbf{N}$, $g(n) \geqq \lfloor \log_2 n \rfloor + 2$ とする．このとき，非線形変換 N_0 を模倣する，$g(n)+3$ 個のセルを使用する k テープ QTM M_2 が存在すれば，与えられたブール式 f が充足可能であるか否かを $O(g(n))$ 個のセルを用いて判定する k テープ DTM M_0 が存在する.

証明：定理 4 より，N_0 を模倣する，$g(n)+3$ 個のセルを使用する k テープ QTM M_2 が存在すれば，任意の i $(1 \leqq i \leqq n)$ に対し，非線形変換 N_i を高々 $g(n)+3$ 個のセルを使用して模倣する k テープ QTM M_{i+4} を構成することができる．よって，高々 $g(n)+3$ 個のセルを使用して $N_1, N_2, \ldots, N_n$ を順に模倣する k テープ QTM M_4 を構成することができる．このような M_4 が存在するので，定理 3 より，与えられた n 変数ブール式 f が充足可能か判定する k テープ DTM M_0 が存在し，M_0 の使用するセルの個数は $O(g(n))$ で押さえられる．■

5 おわりに

本論では，AL アルゴリズムを模倣する QTM の使用するセルの数と，与えられたブール式 f の充足可能性を判定する DTM の使用するセルの数の関係について示した．今後の課題としては，QTM と DTM の領域量の関係についての一般的な結果を導き出すことがあげられる.

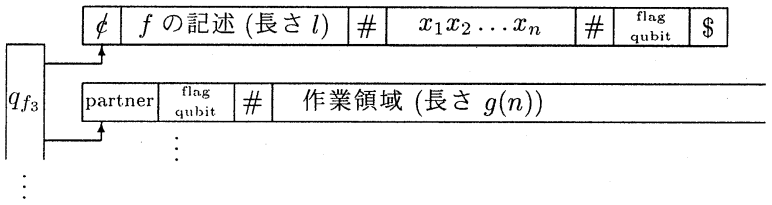

図 4: M_2 が計算を終了して停止したときの様相.

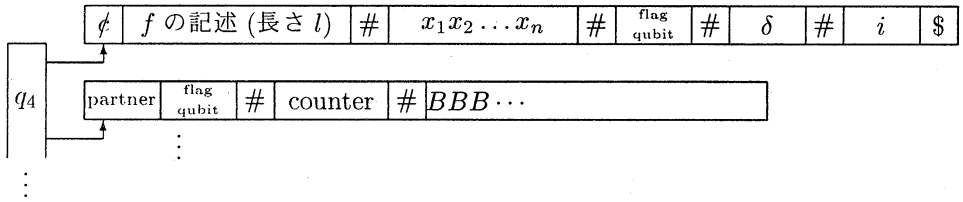

図 5: M_3 が M_2 の模倣を開始する直前の様相.

参考文献

[1] D. S. Abrams and S. Lloyd. Nonlinear quantum mechanics implies polynomial-time solution for NP-Complete and #P Problems. http://arxiv.org/abs/quant-ph/9801041, January 1998.

[2] C. H. Benett. Logical reversibility of Computation. *IBM J.Res.Develop.*, 17:525–532, 1973.

[3] E. Bernstein and U. Vazirani. QUANTUM COMPLEXITY THEORY. *SIAM Journal on Computing*, 26(5):1411–1473, October 1997.

[4] D. Deutsch. Quantum Theory,the Church-Turing principle and the universal quantum computer. *Proc. Royal Soc. London*, A 400(5):73–90, 1985.

[5] L. K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. *Phys.Rev.Lett.*, 79:325–328, 1997.

[6] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[7] M. Ozawa and H. Nishimura. Local Transition Functions of Quantum Turing Machines. http://arxiv.org/abs/quant-ph/9811069, November 1998.

[8] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[9] 金田 直樹 西野 哲朗. NP 完全問題に対する非線形量子アルゴリズムの線形領域シミュレーション. Technical Report COMP98-41, IEICE, Oct. 1998.